

# **Redes de Computadores**





# Material Teórico



Topologias

**Responsável pelo Conteúdo:**

Prof. Esp. Hugo Fernandes

**Revisão Textual:**

Prof. Ms. Luciano Vieira Francisco



# UNIDADE

## Topologias



- Topologias
- Ethernet
- Segurança em Ambiente de Redes



### OBJETIVO DE APRENDIZADO

- Estudar o que são e quais são as topologias disponíveis em redes de computadores locais.
- Tratar da tecnologia ethernet, suas características, funcionalidades, protocolos e meios de transmissão.
- Conhecer alguns outros aspectos, como endereço físico e autonegotiação.





# Orientações de estudo

Para que o conteúdo desta Disciplina seja bem aproveitado e haja uma maior aplicabilidade na sua formação acadêmica e atuação profissional, siga algumas recomendações básicas:



## Assim:

- ✓ Organize seus estudos de maneira que passem a fazer parte da sua rotina. Por exemplo, você poderá determinar um dia e horário fixos como o seu “momento do estudo”.
- ✓ Procure se alimentar e se hidratar quando for estudar, lembre-se de que uma alimentação saudável pode proporcionar melhor aproveitamento do estudo.
- ✓ No material de cada Unidade, há leituras indicadas. Entre elas: artigos científicos, livros, vídeos e sites para aprofundar os conhecimentos adquiridos ao longo da Unidade. Além disso, você também encontrará sugestões de conteúdo extra no item **Material Complementar**, que ampliarão sua interpretação e auxiliarão no pleno entendimento dos temas abordados.
- ✓ Após o contato com o conteúdo proposto, participe dos debates mediados em fóruns de discussão, pois irão auxiliar a verificar o quanto você absorveu de conhecimento, além de propiciar o contato com seus colegas e tutores, o que se apresenta como rico espaço de troca de ideias e aprendizagem.

# Topologias

A topologia, em redes de computadores, está relacionada à forma como as interfaces são conectadas umas às outras. Essa característica define o seu tipo, a eficiência da rede e sua velocidade. Assim, exploraremos as seguintes topologias: totalmente ligada – *full mesh* –, parcialmente ligada – *partial mesh* –, barramento, ponto a ponto, multiponto e estrela.

## Totalmente Ligada – *Full Mesh*

Esta topologia caracteriza-se pela conexão de todas as máquinas da rede, duas a duas, por um meio de comunicação físico. A Figura abaixo ilustra uma rede com topologia totalmente ligada:

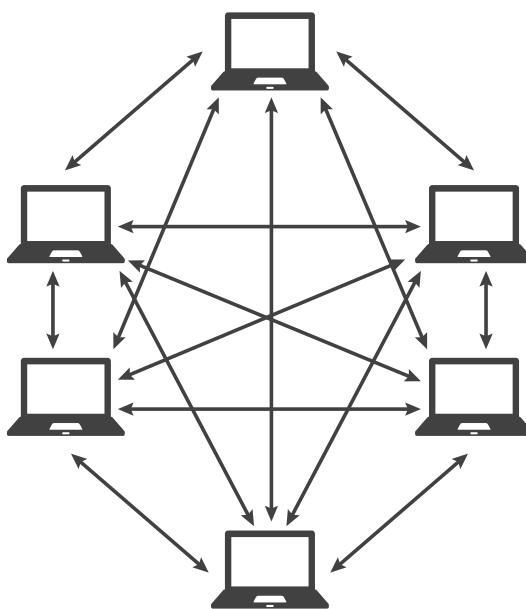


Figura 1 – Topologia totalmente ligada

Fonte: Adaptado de iStock/Getty Images

Essa topologia, embora seja possível sua implementação, não é comumente usada em redes LAN, o que a torna inviável. Isso porque a quantidade de cabos para interligar uma máquina a outra cresce extremamente rápido a partir do momento em que outra máquina é inserida na rede. A fórmula para calcular a quantidade de cabos para uma rede desse tipo é:

$$\text{Qtde\_fios} = (n \cdot (n - 1)) / 2$$



### Trocando ideias...

Portanto, para interligar três equipamentos, precisaremos de três cabos; para interligar quatro equipamentos, precisaremos de seis cabos; e, para interligar dez equipamentos, serão necessários quarenta e cinco cabos. Como se percebe, a quantidade de cabos não cresce linearmente em relação ao número de máquinas e isso torna impraticável o uso desse tipo de rede.

## Topologia Parcialmente Ligada

Neste tipo de tecnologia, os computadores são interligados de forma intermediária, ou seja, não são todos os computadores que são interligados. Portanto, em caso de problemas com a conexão física, há caminhos alternativos para se chegar até a outra máquina. A Figura abaixo ilustra uma topologia parcialmente interligada:

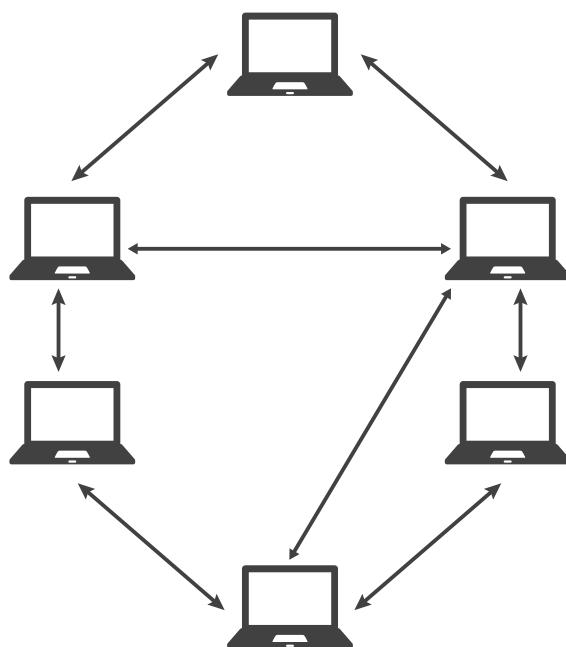


Figura 2 – Topologia parcialmente ligada

Fonte: Adaptado de Istock/Getty images

## Topologia em Barramento

Este tipo de topologia consiste em ter um meio de comunicação comum, ou seja, todos os computadores são conectados a esse meio para estabelecer comunicação entre si. A Figura abaixo demonstra esse tipo de topologia:

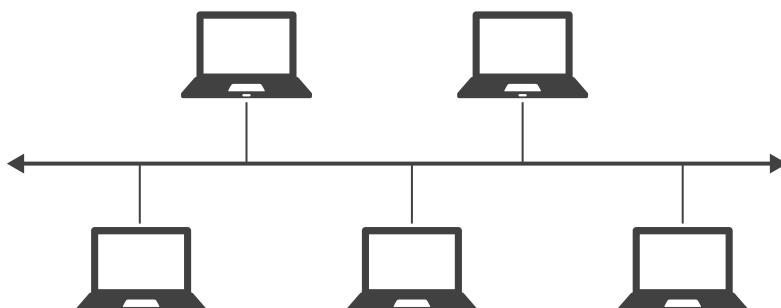


Figura 3 – Topologia em barramento

Fonte: Adaptado de Istock/Getty images

Os computadores são conectados ao meio por uma interface cuja responsabilidade é detectar os sinais transmitidos pelos computadores e tratá-los para que sejam devidamente entendidos pela máquina destinatária.

## Topologia Ponto a Ponto

Este tipo de topologia caracteriza-se por enviar os dados apenas em um sentido como, por exemplo, sentido anti-horário. Conforme se pode ver na Figura abaixo, a interligação entre os computadores é feita nas interfaces de cada máquina. Dessa forma, os dados transmitidos deverão passar pelos computadores até alcançarem o seu destino.

A desvantagem desse tipo de topologia está na quantidade intermediária de pontos entre a máquina de origem e a de destino. Isso passa a ser um problema, pois caso uma dessas máquinas intermediárias apresente problemas, a comunicação ficará prejudicada por não haver caminhos alternativos.

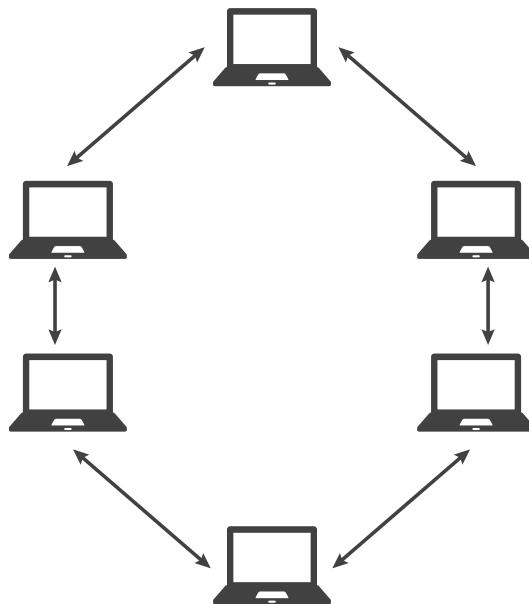


Figura 4 – Topologia ponto a ponto

Fonte: Adaptado de Istock/Getty images

## Topologia Multiponto

Este tipo de topologia é também conhecido como *token ring*. Caracteriza-se por circular no anel, um conjunto padrão de oito bits, chamado de *token*. Quando uma das máquinas tiver que transmitir alguma informação, deverá capturar esse *token* e transmitir os dados. Após a transmissão dos dados, a máquina deverá inserir o *token* novamente no anel. Tal mecanismo é executado para que não haja colisão dos dados a serem transmitidos, pois só poderá transmitir os dados a máquina que conseguir capturar o *token*; aquela que não conseguir, deverá esperar. A Figura abaixo ilustra uma topologia multiponto:

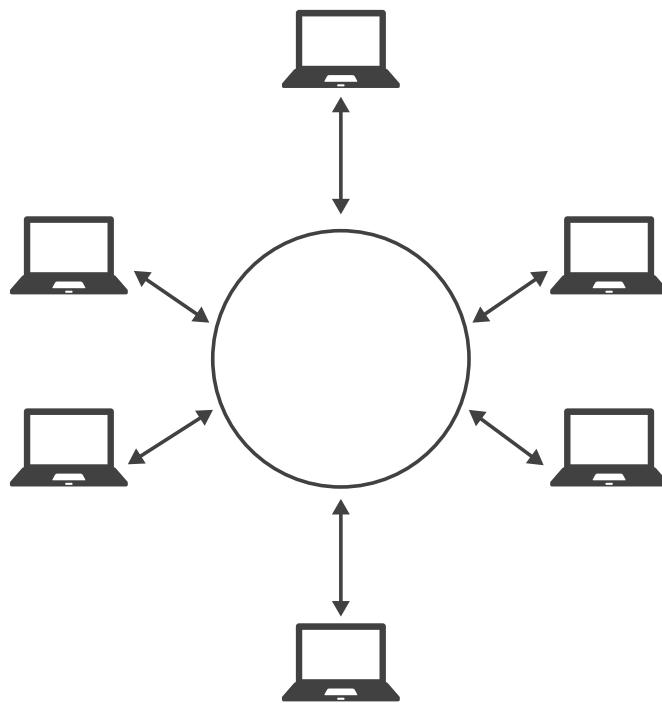


Figura 5 – Topologia multiponto

Fonte: Adaptado de Istock/Getty images

## Topologia em Estrela

---

Caracteriza-se por ter um ponto central para interligar os computadores a fim de estabelecer comunicações. O ponto central age como centro de controle da rede, interligando todas as máquinas. É a topologia mais usual nas redes de computadores LAN e, geralmente, o ponto central é composto por equipamentos do tipo *switch*. Tais equipamentos usam técnicas eficazes para evitar colisões entre os pacotes e outras para aumentar a eficiência da rede.

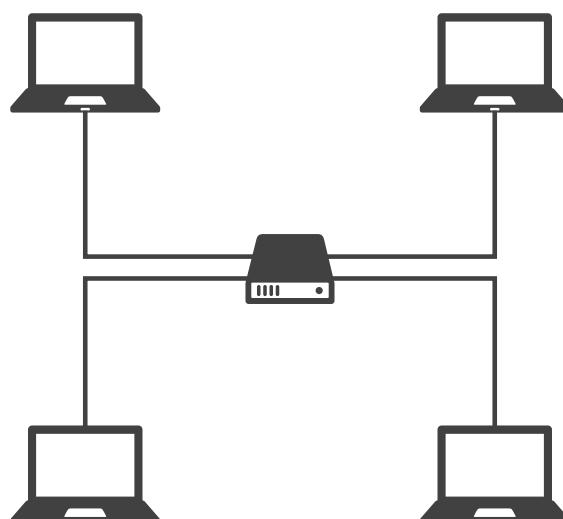


Figura 6 – Topologia em estrela

Fonte: Adaptado de Istock/Getty images

# Ethernet

A *ethernet* constitui um conjunto de protocolos e técnicas para tornar viável a comunicação entre os computadores. É usada na grande maioria das redes de computadores LAN instaladas pelo mundo. Muitas vezes, o termo *ethernet* é empregado para definir as redes locais. Estudaremos as características dessa rede amplamente disseminada.

## História da Ethernet

---

O engenheiro Bob Metcalfe e o doutor Boggs desenvolveram a *ethernet* no início de 1972. Na década de 1980, a tecnologia foi padronizada pelo *Institute of Electrical and Electronics Engineers* (IEEE) com a especificação IEEE 802.3, a qual faz referência à transmissão de dados em baixo nível, considerando o modelo de referência OSI, que é usado para padronização física, elétrica e de protocolos de redes. Entre as características padronizadas, estão a transmissão de dados, protocolos, detalhes técnicos que são usados por fabricantes de placa de redes e cabos a fim de proporcionar compatibilidade entre os equipamentos.

A tecnologia *ethernet* evoluiu durante um longo período de tempo. Devido à padronização, os administradores de redes podem se sentir seguros em adquirir produtos de fabricantes diferentes, pois esses produtos são compatíveis entre si.

Atualmente, navegamos pela internet, participamos de videoconferências, recebemos fluxos de áudio e vídeo e usamos aplicações diversas pela internet. Você já deve ter notado que, a cada dia, necessitamos de velocidades de transmissão maiores para usar aplicações que demandam maior largura de banda. Outro exemplo que demonstra claramente a necessidade de redes locais com maior velocidade é a tecnologia de discos rígidos, que proporcionou respostas mais rápidas para acesso às informações. Há trinta anos, o acesso a um disco remoto teria como problema a velocidade do próprio disco rígido. Hoje, os discos são muito mais rápidos e o acesso a um disco remoto, contendo grande volume de informações, traria problemas para uma rede com capacidade de 10 Mbps. Ao longo das últimas três décadas, a tecnologia *ethernet* tem sido oferecida em velocidades de 1 Mbps, 3 Mbps, 10 Mbps, 100 Mbps e 1 Gbps (1.000 Mbps). Em consequência do aumento da velocidade, vários meios físicos são utilizados para trafegar dados pela tecnologia *ethernet* como, por exemplo, cabos coaxiais grossos, cabos coaxiais finos, várias categorias de pares trançados e fibras ópticas.

Uma das mudanças na tecnologia *ethernet*, que impediu sua aposentadoria, diz respeito à facilidade de uso e custo. A *ethernet* original usava um cabo coaxial grosso e apresentava duas desvantagens: uma das quais era a dificuldade de instalação; a outra estava no cabo coaxial, que passava de equipamento em equipamento, fazendo com que qualquer interrupção no cabo resultasse na parada total da rede inteira. Para resolver esses efeitos, outras mídias foram utilizadas.

Primeiro, o uso do cabo coaxial fino, que apresentava uma flexibilidade maior em relação ao cabo coaxial grosso; com isso, foi resolvida a questão de instalação. Segundo, para resolver a questão de interrupção, criou-se um equipamento chamado repetidor, ao qual todos os equipamentos se conectavam através de um cabo de par trançado. Dessa forma, a interrupção de sinal em um cabo de par trançado só afetaria a comunicação com um equipamento – e não com a rede inteira, como ocorria com o cabo coaxial. Para possibilitar velocidades mais altas, várias “categorias” de cabos de par trançados surgiram.

Para uma velocidade ainda maior e para atingir distâncias maiores nas redes *ethernet*, a fibra óptica foi introduzida. Essas capacidades são possíveis, pois a fibra óptica é imune a ruídos.

A tecnologia *ethernet* foi padronizada em 1985 pelo IEEE, sob o padrão de número 802.3. Os padrões DIX e IEEE 802.3 são ligeiramente diferentes. Com o tempo, outros padrões foram criados para acomodar velocidades crescentes e meios físicos variados.

## Princípios de Operação

Estudaremos, abaixo, alguns princípios de operação da tecnologia *ethernet*. Tais princípios serão de grande valor.

### Endereçamento

Em um nível de abstração mais alto, pode-se dizer que a tecnologia *ethernet* oferece a comunicação entre equipamentos de uma mesma rede física sem o uso de conexões e com serviços:

- *Unicast*, ou seja, um quadro *ethernet* vai para um destino único. Analogamente, pode-se tomar como exemplo o envio de um *e-mail* para uma única pessoa; o *e-mail* é direcionado;
- *Multicast*, em que um quadro vai para múltiplos destinos. Analogamente, pode-se tomar como exemplo o envio de um *e-mail* para um grupo de pessoas; portanto, um *e-mail* é distribuído para um grupo de pessoas;
- *Broadcast*, em que um quadro vai para todos os destinos, ou seja, o quadro é enviado para todas as máquinas de uma mesma rede.



Veja alguns exemplos práticos do uso de cada um desses pacotes:

- **Unicast** – os protocolos que usam unicast são: HTTP, SMTP, FTP e Telnet;
- **Multicast** – é bastante usado em teleconferências, onde um emissor fala com vários receptores ao mesmo tempo;
- **Broadcast** – como exemplo, a consulta de resolução de endereço que o protocolo Address Resolution Protocol (ARP) envia para todos os endereços na LAN.

Para concretizar esses serviços, cada componente de rede participante da comunicação possui um endereço único, chamado de *endereço MAC*, ou *endereço físico*. Os endereços MAC possuem 48 bits e são únicos por interface de rede; significa que, quando um fabricante desenvolve uma placa de rede *ethernet*, recebe um endereço único determinado por *hardware*. Não se utilizam subcampos do endereço MAC para determinar a localização geográfica ou para ajudar no encaminhamento da informação. Uma interface de rede com o endereço MAC 00-07-95-03-FA-89 – em hexadecimal – poderia estar no Brasil, enquanto a interface com o endereço 00-07-95-03-FA-8A poderia estar em outra rede local, por exemplo, na China.

Embora o assunto não tenha relação com a tecnologia *ethernet* em si, é útil lembrar que, no momento em que duas estações conectadas à rede querem se comunicar, a máquina de origem conhece o endereço IP da máquina de destino, mas ainda não conhece seu endereço MAC. O mapeamento de endereços IP para endereços MAC é feito com o protocolo ARP.

A *ethernet* permite que quadros sejam enviados para endereços especiais. O endereço FF-FF-FF-FF-FF-FF é o de *broadcast*. O quadro enviado para tal endereço é recebido por todas as máquinas de uma rede *ethernet*. Ademais, cada interface de rede – placa de rede – pode ser configurada para receber quadros pertencentes a um grupo *multicast*.

### Quadro *Ethernet*

Embora haja uma pequena diferença na organização do quadro entre o padrão DIX desenvolvido pela Xerox e o padrão IEEE 802.3, o protocolo IP utiliza o quadro IEEE 802.3 de forma compatível ao padrão DIX. Todos os pacotes pertencentes a um protocolo têm um cabeçalho que ajuda os equipamentos da rede a transportá-los. O quadro *ethernet* também tem campos que são usados para o mesmo objetivo. O conhecimento da organização do quadro não é importante para o usuário final. Partindo desse pressuposto, podemos destacar somente alguns pontos importantes:

- O quadro *ethernet* contém os endereços físicos – MAC – das estações de origem e de destino;
- Ao transportar pacotes IPv4, o campo *tipo* receberá o valor hexadecimal 0x0800; para IPv6, o tipo é 0x86DD; para ARP, é 0x0806. O tamanho mínimo do quadro – sem incluir o preâmbulo – é de 64 bytes e o tamanho máximo é de 1.518 bytes;
- O quadro possui um campo de verificação – chamado de *Frame Check Sequence* (FCS), ou *Cyclic Redundancy Check* (CRC) –, permitindo que a estação de destino detecte erros na transmissão.

## Protocolo MAC

Conceitualmente, uma rede *ethernet* simples consiste de um barramento único que todas as máquinas querem acessar para realizar suas transmissões de dados. Como esse meio é único e compartilhado, apenas uma estação pode transmitir em um determinado período de tempo, portanto, a comunicação é considerada *half-duplex*. Considerando essa característica, deve haver uma forma de organizar o acesso ao meio, de modo que cada estação possa, eventualmente, transmitir um quadro de cada vez. O protocolo que realiza esse controle chama-se *Media Access Control* (MAC).

A *ethernet* usa um mecanismo bastante simples para realizar o acesso ao meio, o qual recebeu o nome de *Carrier-Sense Multiple Access with Collision Detection* (CSMA-CD), ou acesso múltiplo usando detecção de portadora e detecção de colisão, funcionando da seguinte maneira: quando uma estação quer transmitir informação no meio compartilhado, por exemplo, o cabo de par trançado, espera até verificar que um sinal chamado de portadora esteja ausente – indicando que ninguém está transmitindo naquele momento. Inicia, então, sua transmissão. Como outra estação pode ter tomado a mesma decisão, é possível que haja uma colisão, situação em que as transmissões interferem uma na outra. Cada estação é informada sobre a colisão e para de transmitir. As máquinas esperam por certo tempo aleatório antes de tentar transmitir os dados novamente. Cada máquina poderá transmitir sem interferência das demais máquinas e, se houver colisão, o procedimento é novamente repetido. É importante observar que as colisões são eventos absolutamente normais em uma rede *ethernet*, no entanto, um excesso de colisões pode diminuir sensivelmente o desempenho da rede.

## Ethernet Full-Duplex

O protocolo CSMA-CD descrito no item anterior permite acesso múltiplo ao meio de transmissão, resultando em comunicação *half-duplex*: não há transmissões simultâneas no meio. Sob certas circunstâncias, é possível operar em modo *full-duplex*, ou seja, com duas estações transmitindo simultaneamente. Isso é possível sempre que a configuração da rede permitir que, no máximo, duas fontes possam transmitir no meio ao mesmo tempo. Dito de outra forma, a comunicação *full-duplex* dobra a capacidade do enlace. Por exemplo, um enlace que, no modo *half-duplex*, possui capacidade total de 100 Mbps, passa a ter capacidade de 100 Mbps em cada sentido se estiver operando em modo *full-duplex*.

Raciocinando um pouco mais, podemos concluir imediatamente que, já que não há acesso múltiplo a um enlace *full-duplex*, não há necessidade de usar o mecanismo CSMA-CD. De fato, o modo de operação *full-duplex* desabilita o mecanismo CSMA-CD da tecnologia *ethernet*. Os equipamentos envolvidos podem transmitir quando querem, sem detectar a portadora nem verificar colisões. Na realidade, colisões nunca ocorrem em modo *full-duplex*.

Terminaremos a discussão sobre o modo *full-duplex* com um alerta: não basta ter comunicação ponto a ponto para que o modo *full-duplex* seja habilitado. Ambos os lados devem ser configurados para esse modo de operação, seja através de um procedimento manual ou de autonegociação. Não se pode misturar os modos *half-duplex* e *full-duplex* em cada lado do enlace, pois isso resultaria em erros de vários tipos, incluindo mais colisões e erros.

## Autonegociação

O desenvolvimento da tecnologia *fast ethernet* de 100 Mbps, em 1995, aumentou não apenas a velocidade dos enlaces *ethernet*, mas também trouxe transtornos provenientes de misturas das tecnologias de 10 e 100 Mbps em interfaces compatíveis. É possível, por exemplo, usar o mesmo par trançado para o tráfego de 10 ou 100 Mbps, além de o mesmo ser aplicado em fibras ópticas. Outro complicador é a existência de placas de rede 10/100 e 10/100/1000 e equipamentos de interconexão que podem funcionar tanto a 10 quanto a 100 ou 1.000 Mbps. Portanto, ao conectar um equipamento a um *switch ethernet* ou repetidor, é necessário tornar compatível a velocidade de operação e o modo de operação – *half-duplex* ou *full-duplex*. Essa compatibilidade pode ser feita manual ou automaticamente através do mecanismo de autonegociação, como dito, introduzido em 1995 nas tecnologias *ethernet*. Quando ambos os lados de um enlace possuem suporte à autonegociação, escolhem a combinação de parâmetros que dará melhor desempenho. Isto é, a maior velocidade possível é escolhida – 10, 100 ou 1.000 Mbps – e o modo *full-duplex* é selecionado, caso seja suportado por ambos os lados.

Devido à existência de *hardware* antigo, ocorrem casos em que um lado, digamos o lado **A**, oferece suporte à autonegociação, enquanto o outro lado, o **B**, não dá suporte à autonegociação. Nesse caso, **A** perceberá que **B** não está fazendo autonegociação e passará a fazer detecção paralela. Nesse mecanismo, **A** descobre a velocidade de **B** e, obrigatoriamente, escolhe o modo de operação *half-duplex*. Dois problemas associados à detecção paralela podem ocorrer na prática:

- O lado **B** não oferece suporte à autonegociação, mas foi manualmente configurado em modo *full-duplex*. Nesse caso, o lado **A** escolherá *half-duplex* e a comunicação não ocorrerá de forma satisfatória;
- O lado **A** implementará a autonegociação, mas não implementará o padrão corretamente e escolherá o modo de operação *full-duplex*. A solução para este caso será atualizar a versão do *driver* da placa de rede ou do *software* do equipamento de interconexão. A autonegociação existe apenas para mídias de par trançado e para *gigabit ethernet* com fibra óptica; não há opção de autonegociação para *ethernet* em fibra óptica em velocidades de 10 e 100 Mbps – o motivo é que esses equipamentos utilizam feixes de luz de comprimento de onda diferentes, não sendo possível realizar a autonegociação.

## Camada Física da *Ethernet* – Padrões

O meio de transmissão físico de uma LAN com fios envolve cabos, principalmente par trançado ou fibra óptica. Um cabo de par trançado é composto de oito fios, formando quatro pares de fios de cobre torcidos e utilizado com plugues e soquetes RJ-45. O comprimento máximo de um cabo de par trançado é de 100 m, enquanto que para um de fibra óptica, o comprimento máximo varia de 10 a 70 km, dependendo do tipo de fibra. Conforme o tipo de par trançado ou cabos de fibra óptica utilizados, as taxas de dados atuais podem variar de 100 para 10.000 Mbits.

A seguir serão apresentados os padrões do meio físico de transmissão de uma rede LAN.

O nome abreviado do padrão *ethernet* 802.3, segundo o IEEE é composto da seguinte forma:

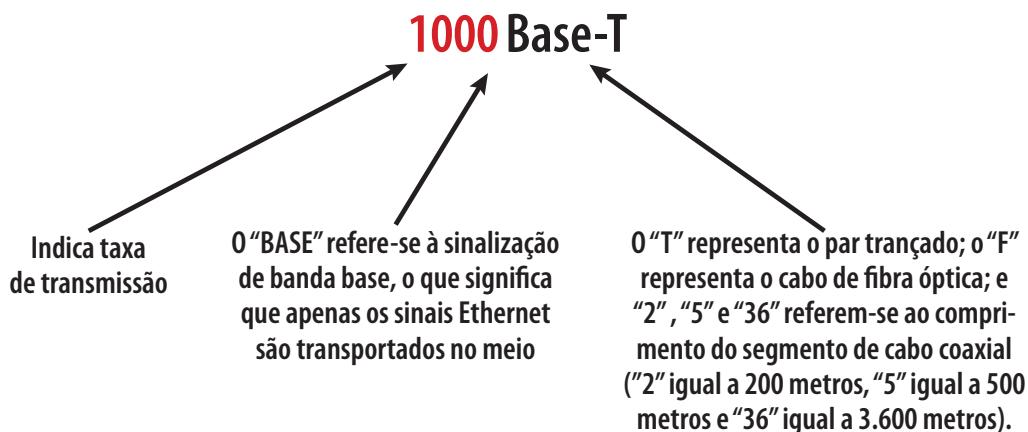


Figura 7

### Padrões 10 BASE-5 e 10 BASE-2

Esses são os dois padrões *ethernet* que utilizam cabo coaxial. Funcionam a 10 Mbps e são consideradas tecnologias obsoletas. Todas as outras tecnologias que não pertencem a 10 BASE-5 e 10 BASE-2 permitem operação em modo *full-duplex*, no entanto, essas duas tecnologias não oferecem transmissão nesse modo. A topologia usada é em barramento e o comprimento máximo do cabo é de 185 m para o BASE-2 e 500 m para o BASE-5.

O 10 Base-2 usa cabo coaxial BNC T, espaçados, no mínimo, 0,5 m para evitar interferências. Uma ponta do cabo termina com um resistor de 50 ohm e a outra ponta precisa ser aterrada. Um segmento é constituído por diversos pedaços de cabo, sendo cada pedaço conectado com um conector T.



Figura 8 – Conector coaxial T

O padrão 10 BASE-5 é conectado através de transceptor e cabo de transceptor, os transceptores são espaçados em até 2,5 m para evitar interferências. A conexão física do transceptor exige a inserção no cabo de uma conexão conhecida como “vampira”. Uma ponta do cabo termina com um resistor de 50 ohm e, como descrito, a outra ponta deve ser aterrada.

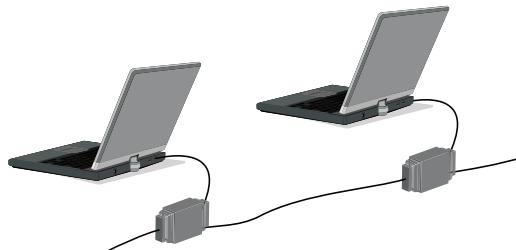


Figura 9 – Conexão da tecnologia 10 Base-5

### Padrão 10 BASE-T

Este padrão popularizou a *ethernet*. A velocidade é padronizada em 10 Mbps e dois pares de fios trançados de categoria três, embora os cabos de categoria cinco sejam largamente utilizados atualmente – mas nesta padronização não foi usado. Os cabos de categoria mais alta apresentam melhor desempenho, pois a cada alteração feita para melhoria de desempenho, os cabos assumem uma versão com um número ou uma letra maior. Os cabos têm comprimento máximo de 100 m, caso a distância seja maior que isto, o equipamento repetidor deve ser usado. A topologia empregada é em estrela e somente dois nós podem ser conectados por segmento – uma estação de trabalho e um equipamento repetidor. Os HUB, switches e placas de rede utilizam conectores modulares de oito pinos (RJ-45).

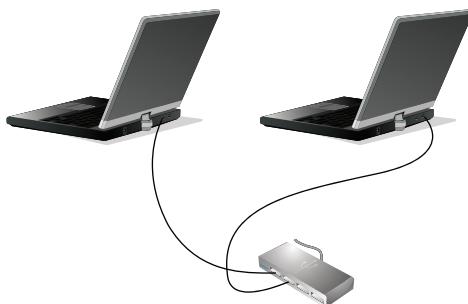


Figura 10 – Conexão da tecnologia 10 Base T

## Padrão 10 BASE-FL

Operando a 10 Mbps, esse padrão usa cabo de fibra óptica multimodo. É uma extensão de um padrão mais antigo, chamado de *Fiber Optic Inter-Repeater Link* (Foirl). A fibra pode ter até 2.000 m de comprimento. Pode ser usada para interconectar estações de trabalho ou repetidoras.

## Padrão 100 BASE-TX

O padrão *fast ethernet* é mais comumente empregado com velocidade de 100 Mbps, usando dois pares de fios trançados de alta qualidade – categoria cinco ou melhor. O cabo está limitado à distância de 100 m, sem uso de repetidor. Usa um sistema de sinais em *duplex* completo e baseado na subcamada dependente do meio físico de par trançado, que é um padrão Ansi em que define a maneira como os dados são codificados e decodificados para transmissão. As redes baseadas no padrão 100 BASE-TX precisam ser inteiramente compatíveis com a categoria cinco, inclusive os cabos e conectores. Como muitas instalações de redes usam cabo de par trançado categoria cinco de quatro pares, uma instalação 100 BASE-TX reserva aos administradores dois pares extras de cabos, que podem ser usados para comunicação de voz ou reservados para melhorias futuras na rede. Atualmente, esses dois pares extras não podem ser usados para dar suporte a outra rede local de alta velocidade.

## Padrão 100 BASE-FX

O padrão *fast ethernet* utiliza fibras ópticas multimodo. A fibra pode ter até 2.000 m de comprimento. Dá suporte às operações de internet de 100 Mbps sobre dois cabos de fibra óptica multimodo; um dos cabos é usado para transmitir dados e o outro para receber dados. A tecnologia 100 BASE-FX compartilha o mesmo sistema de sinalização do 100 BASE-TX, porém, usa para subcamada dependente de meio físico de fibra, a tecnologia FDDI. Diferentemente do que temos nas tecnologias 100 BASE-TX, os segmentos 100 BASE-FX são conhecidos como segmentos de ligação e são projetados para conectar somente dois nós em uma topologia ponto a ponto. Consequentemente, a aplicação básica do 100 BASE-FX é no *backbone* e este é usado para conectar HUB de *fast ethernet*.

## Padrão Gigabit Ethernet

Ao longo do tempo, surgiram aplicações “sedentas” por largura de banda; a integração de sistemas computacionais mais rápidos e a migração da *fast ethernet* dos *backbones* para a LAN criaram “gargalos” para o servidor e para as conexões comutadas. O *gigabit ethernet* alivia esse congestionamento, tornando-se uma tecnologia mais rápida para o *backbone*. Lembre-se, quando a *ethernet* foi desenvolvida, a maioria das aplicações em sistemas computacionais não podia saturar um canal de 10 Mbps. Hoje, contudo, temos servidores de 64 bits de barramentos, velocidade de barramento aumentada, computadores de mesa de 100 Mbps, aplicações em tempo real e conferências de vídeo, além de voz sobre IP e aplicações multimídia.

## Padrão 1000 BASE-T

O *gigabit ethernet* funciona a 1.000 Mbps – 1 Gbps – e utiliza quatro pares de fios trançados de categoria cinco ou melhor. Como ocorre na maioria dos padrões *ethernet*, o comprimento máximo do cabo é de 100 m.

## Padrão 1.000 BASE-X

Este padrão de *gigabit ethernet* utiliza fibra óptica e é largamente utilizado em *backbones* de redes de campus/prédios. A fibra pode ter até 220 m de comprimento se for multimodo e até 5.000 m se for monomodo.

## Metro Ethernet

*Metro ethernet* é uma tecnologia que permite utilizar redes *ethernet* em áreas metropolitanas e geograficamente distribuídas. Esse conceito surgiu porque, de acordo com alguns estudos, o tráfego de dados estaria superando o tráfego de voz nas redes metropolitanas, portanto, seria mais interessante utilizar uma infraestrutura de transmissão de dados do que uma *Time Division Multiplexing* (TDM), criada para a transmissão de voz.

O esquema básico do serviço *metro ethernet* é ilustrado abaixo. O provedor da *Metro Ethernet Network* (MEN) provê o serviço *metro ethernet* aos seus clientes. O Cliente (CE) é conectado à MEN por meio da interface de rede do Usuário (UNI).

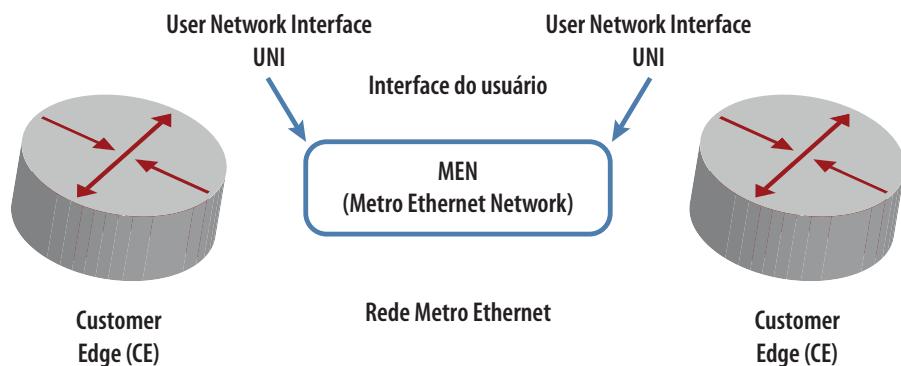


Figura 11 – *Metro ethernet*

O provedor da rede *metro ethernet* pode oferecer serviços baseados em diversas tecnologias e protocolos, como Sonet, WDM, MPLS, Frame Relay, SDH etc., mas sob a perspectiva do assinante, a conexão é sempre feita por meio de uma interface *ethernet* comum.

Segundo Marco Filippetti (2008), a rede *metro ethernet* oferece as seguintes vantagens para provedores e assinantes:

- Não necessita de roteador ao lado do cliente, diminuindo o custo sobre equipamentos;
- Flexibilidade para aumento de largura de banda por demanda;

- Fácil manutenção;
- Fácil gerenciamento;
- Equipamentos com custos mais baixos do que nas redes mais “antigas” – ATM, Sonet, FR etc.;
- Do lado do cliente não são feitas grandes alterações, pois usará uma interface *ethernet* comum e bem conhecida, integrando-se perfeitamente à LAN já instalada;
- Flexibilidade ao provedor para oferecer serviços de valor agregado;
- Maior largura de banda para os clientes do que outras tecnologias – como DSL ou *cable modems*;
- Possibilidade de o cliente pagar apenas pela banda utilizada – fácil implementação desse controle no lado da operadora.

Para que você tenha ideia, um usuário com serviço de banda larga com velocidade de 8 Mbps tem uma capacidade muito boa para trafegar na internet. Agora, se considerarmos que uma rede LAN tem capacidade de trafegar dados na velocidade de 1.000 Mbps, então 8 Mbps é considerada uma conexão baixa. Portanto, quando trocamos dados entre os computadores que estão na mesma rede, usamos, aproximadamente, a taxa determinada nas interfaces de rede; mas, se acessarmos a internet, essa taxa baixará de acordo com a velocidade do serviço contratado junto à operadora telefônica. Se a tecnologia *ethernet* já estivesse em sua plena implementação, poderíamos chegar a uma taxa próxima à da velocidade oferecida pela operadora de telefonia.

## Segurança em Ambiente de Redes

Com ataques de *crackers* e a proliferação de vírus, a maioria das pessoas concorda que a segurança dos dados é uma das questões mais importantes hoje em dia. Toda a organização requer um conjunto de *softwares* e até equipamentos para prover segurança, mas poucas têm uma boa compreensão de como conseguir.

Há muitas maneiras de conseguir diversos níveis de segurança de redes, entretanto, tais métodos podem ser extremamente caros ou podem não proteger completamente os usuários de muitos perigos que surgem diariamente. A implementação apropriada de segurança de rede não é trivial, nem barata e requer experiência que engloba a maioria das áreas de Ciência da rede.

Os *crakers* usam ferramentas que procuram por vulnerabilidade na rede, no *hardware* e até em sistemas operacionais. Várias iniciativas devem ser colocadas em prática para minimizar o risco de invasão, mas nada adianta ter soluções tecnológicas sofisticadas, integradas a parceiros nos clientes e fornecedores se não há restrições, políticas e processos que estabeleçam e organizem a conduta do profissional dentro da corporação para minimizar esse tipo de problema. A

empresa deve implementar uma boa política de uso dos recursos de informática e, periodicamente, atualizar todos os funcionários em relação a essa política e, também, em treinamentos.

Outro fator relevante em relação à segurança são as senhas.

As senhas de um funcionário podem ser facilmente descobertas, mesclando itens comuns como o nome e sobrenome, data de aniversário, nome de esposa, filho etc. As senhas que são difíceis de adivinhar incluem uma mistura de letras maiúsculas e minúsculas, dígitos, sinais de pontuação e caracteres especiais e têm, normalmente, sete ou oito caracteres de comprimento. Abaixo encontram-se três sugestões para a criação de senhas fortes:

- Misture as primeiras letras de uma frase fácil de lembrar, com dígitos, sinais de pontuação ou caracteres especiais;
- Combine duas palavras relativamente curtas com algum caractere especial, dígito ou sinal de pontuação;
- Use letras, caracteres especiais e sinais de pontuação para representar uma sentença em inglês.

Adote como regra alterar a senha, no mínimo, a cada seis meses e tenha em mente que um usuário com uma senha fraca pode comprometer a segurança de uma rede inteira.

Você já percebeu que muitos fornecedores de *software* oferecem uma versão padrão que facilita a instalação. Muitos oferecem facilidades na instalação porque não são todos os usuários que têm conhecimento para uma instalação personalizada. Embora esse procedimento seja conveniente para alguns usuários, permite espaço para vulnerabilidades. Geralmente, as instalações *default* incluem *script* ou programas de exemplos que, muitas vezes, poderiam ser descartados. Você sabia que uma das vulnerabilidades mais sérias relacionadas a servidores *web* diz respeito aos *scripts* de exemplos, os quais são utilizados por invasores para penetrar o sistema? As recomendações básicas para maior segurança são as seguintes:

- Remova softwares desnecessários;
- Desabilite serviços fora de uso;
- Bloqueie portas não usadas.

A tecnologia sem fio vem crescendo não apenas entre as empresas, mas também entre os usuários domésticos. Os equipamentos móveis são, realmente, tecnologias emergentes. Assim, tome cuidado com a facilidade de instalação desses dispositivos. Muitas vezes essa facilidade está vinculada a várias vulnerabilidades por não haver necessidade de implementar uma configuração mais minuciosa.

Infelizmente, os sistemas operacionais são desenvolvidos e colocados no mercado com algumas falhas. A partir do momento em que algumas vulnerabilidades são encontradas, os fornecedores desses sistemas operacionais disponibilizam, de forma gratuita, as atualizações. É extremamente interessante deixar habilitada,

nesses sistemas operacionais, a opção de atualização automática. Desta forma, ao se conectar à internet, o sistema operacional, automaticamente, procurará por essas atualizações e as implementará, a fim de eliminar eventuais vulnerabilidades.

Para evitar que pessoas não autorizadas accessem a rede de computadores, deve-se instalar uma unidade de *hardware* ou *software* chamada *firewall*, a qual permite controlar as comunicações bidirecionais utilizando uma política de segurança específica. Detecta intrusões, além de permitir, através de regras bem definidas, o que pode ou não ser acessado na internet. Há softwares *firewall* gratuitos que podem ser baixados pela internet e instalados nos computadores; dessa forma, é possível restringir o acesso de pessoas não autorizadas à rede e, consequentemente, ao seu computador.

Dependendo do grau de importância da informação para uma empresa, há necessidade de se instalar dispositivos biométricos para acesso a determinadas áreas. Biometria é o ramo da Ciência que estuda as medidas físicas dos seres vivos. A tecnologia biométrica é utilizada para a identificação de pessoas através das características únicas de cada indivíduo, como a face, a íris e a impressão digital.

O que se pode perceber é que as informações de uma empresa, sendo de pequeno, médio ou grande porte, têm valor significativo para a continuidade dessa em um mercado cada vez mais competitivo. Tais informações estão, hoje, digitalizadas, portanto, as organizações devem adotar, cada qual de acordo com a própria necessidade, formas de segurança para que essas informações não caiam em mãos erradas.



Sobre esse assunto, leia o seguinte capítulo – disponível na Biblioteca Virtual Universitária: KUROSE, J.; ROSS, K. W. Segurança em redes de computadores. In: **Redes de computadores e a internet: uma abordagem top-down**. 6. ed. [S.l.: s.n., 20--?].

## Backup

As tecnologias de *backup* e recuperação são a base das estratégias de proteção de dados que ajudam as empresas a atender aos seus requisitos de disponibilidade e acessibilidade de dados.

A empresa deve adotar uma estratégia para *backup*. Muitas vezes o administrador pode se sentir tentado a executar *backup* de todos os servidores do ambiente. No entanto, lembre-se de que o objetivo é poder restaurar, com êxito, o ambiente depois de uma pane ou um desastre. Portanto, em linhas gerais, a estratégia da empresa deve concentrar-se em objetivos como:

- Os dados a serem restaurados devem ser fáceis de localizar;
- A restauração deve ser feita o mais rapidamente possível.

Se o administrador fizer *backup* de todo o servidor sem utilizar uma metodologia, terá um grande volume de dados a recuperar.

Quanto mais arquivos forem incluídos no *backup*, mais demorada será a recuperação dos quais. Se ocorrer um desastre, o tempo para recuperação será determinante, pois essa ação deverá ser aplicada o mais rápido possível.

*Backups* podem ser feitos de forma *on-line*, tendo como característica a possibilidade de se fazer cópias dos arquivos sem a necessidade de interrupções do sistema. Normalmente, são usados por aplicativos que devem estar disponíveis vinte e quatro horas por dia, como, por exemplo, servidores de *e-mail* e bancos de dados.

A vantagem do *backup on-line* é que, além da não interrupção do serviço, os aplicativos e dados permanecem totalmente disponíveis para os usuários durante o processo de *backup*. Assim, os *backups on-line* podem ser agendados durante o horário de funcionamento normal das empresas.

Como desvantagem, há o fato de que, durante o processo de *backup*, o desempenho pode ser prejudicado em servidores de produção e, dependendo dos aplicativos que estiverem ativos durante o processo, pode não ser feito o *backup* de alguns arquivos de dados abertos.

Em contrapartida, há a possibilidade de se fazer o *backup off-line*, o qual é executado colocando-se o sistema e os serviços *off-line*.

As vantagens do *backup off-line* é que você pode ter um melhor desempenho, uma vez que o servidor pode se dedicar à tarefa exclusiva de *backup*. Além disso, todos os arquivos são copiados, pois, neste caso, não haverá arquivos abertos durante o processo.

Como desvantagem fica a não disponibilidade dos arquivos para os usuários enquanto o processo de *backup* estiver em execução.

# Material Complementar

## Indicações para saber mais sobre os assuntos abordados nesta Unidade:

### Livros

#### **Redes de Computadores e a Internet: Uma Abordagem Top-Down**

KUROSE, J.; ROSS, K. W. **Redes de computadores e a internet: uma abordagem top-down.** 6. ed. [S.l.: s.n., 20--?]. cap. 1.

### Leitura

#### **Segurança em Redes de Computadores**

SOUZA, W. Segurança em redes de computadores. **Brasil Escola**, [20--].

<https://goo.gl/2gn8Xm>

#### **Padrões Ethernet, parte 1: 10 e 100 megabits**

MORIMOTO, C. E. **Padrões ethernet, parte 1: 10 e 100 megabits.** 9 jan. 2008.

<https://goo.gl/sM4en8>

#### **Ethernet completa 40 anos e um dos Criadores conta sua História**

LAWSON, S. *Ethernet completa 40 anos e um dos criadores conta sua história.* **IDGNow**, 23 maio 2013.

<https://goo.gl/Qmtv0g>

# Referências

ANDREW, S.; TANENBAUM. **Redes de computadores**. 4. ed. São Paulo: Campus, 2003.

FILIPPETTI, M. **Redes metro-ethernet**. 2008. Disponível em: <<http://blog.ccna.com.br/2008/04/27/metro-ethernet>>. Acesso em: 6 jan. 2014.

GALLO, M. A.; HANCOCK, W. M. **Comunicação entre computadores e tecnologias de rede**. São Paulo: Thomson Learning, 2003.

KUROSE, J. F. **Redes de computadores e a internet: uma nova abordagem**. São Paulo: Addison-Wesley, 2004.



**Cruzeiro do Sul Virtual**  
Educação a Distância

www.cruzeirodosulvirtual.com.br  
Campus Liberdade  
Rua Galvão Bueno, 868  
CEP 01506-000  
São Paulo - SP - Brasil  
Tel: (55 11) 3385-3000



**Cruzeiro do Sul**  
Educacional